Information Security Practices

➢ Top Vulnerabilities

➢ Compliance Issues

➢ E-Mail Etiquette

Presented by Debbie Martin
Security Officer

Most Significant Vulnerabilities

In No Particular Order:

➢ Passwords & Logon IDs
➢ Configuration and Documentation
➢ Data.

Passwords

➢ Access Control is **Only** Effective

If We *Make* it Effective

➢ Primary Access Authorization Mechanism

➢ No Sharing…NO EXCEPTIONS.

Passwords

➢ Advocate Strong Passwords

➢ Mandatory Changes – 90 Day Cycle

➢ Protect ALL Passwords

➢ Change Default Passwords.

Logons

➢   Do NOT Share. No Exceptions

➢   Do NOT Leave an Active Session Unattended

➢   Screensaver Password Active on all Computers.

Configuration and Documentation

- Inconsistent & Undocumented Configurations

  ➤ Unauthorized Software and Hardware

  ➤ Unauthorized Access

  ➤ Patches and Updates

  …Eliminate Duplicate and Redundant Work

Software Issues

➢ Licensing and Ownership
➢ Compatibility
➢ Hitchhikers
➢ Support.

Hardware Issues

➢ Ownership

➢ Liability

➢ Support

➢ Compatibility

➢ Control.

Non-CDCR Device or Software Form

- ➢ When To Use
- ➢ Who Must Approve
- ➢ Why
- ➢ Alternatives.

CDs, Diskettes and USB

Controlling Usage –

➢ Disable Drives
➢ Scan *every time*

Unauthorized Access

- ➢ Computers
- ➢ Network Resources
- ➢ Registry
- ➢ Applications
- ➢ Data.

Patches and Updates

Adhere to the standard and configuration
set by
Data Center

You can replace a computer….

but replacing data
is another matter…

Data

➢ Are your Files Important?
   Back Up!

➢ Protecting Data Files…
   Where ever they are

➢ Need to Share Data?
   Do it Securely.

Data Backups

- ➢ Daily or Whenever Changes are Made

- ➢ Dependable Media

- ➢ TEST TEST TEST

- ➢ Storage Locations

- ➢ Using the Network.

Protecting Data Files…Where ever they are

➢ Desktop Computers

➢ Network Shares

➢ Laptop and Notebook Computers

➢ Handhelds and PDAs

➢ Removable Media.

Need to Share? Do it Securely

What "Secure" is **NOT**:

➢ EMAIL
➢ Non-encrypted FTP
➢ Removable Media
➢ "Public" Network Shares.

Need to Share? Do it Securely

What "Secure" IS:

➢ Secure-FTP
➢ Encrypted Data on Removable Media
➢ Limited Access Network Shares.

Compliance Issues

➢ Is it Confidential?

➢ Protecting Confidential Information

➢ User Agreement Forms

➢ Incident Reporting.

Is it Confidential?

- ➢ Information Practices Act
- ➢ HIPAA
- ➢ Public Records Act.

Each agency shall maintain in its records only personal information which is *relevant and necessary* to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government.

California Civil Code, 1798.14

Each agency shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the provisions of this chapter, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury.

California Civil Code, 1798.21

Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

California Civil Code 1798.29

"Personal Information" is defined as…

Last name and First Name or First Initial in combination with any of the following data elements:

- ➤ Social Security Number
- ➤ Drivers License Number
- ➤ Bank Account, credit/debit card numbers.

HIPAA

Protected Health information means individually identifiable health information

Other Confidential Information defined in the Public Records Act

- ➢ Health contracts and related information.
- ➢ Investigatory or security documents from or to law enforcement agencies, including CDCR
- ➢ Information collected under the Evidence Code
- ➢ Correspondence with the Governor or his office
- ➢ Documents pertaining to collective bargaining
- ➢ Vulnerability assessments related to terrorism and other criminal activity
- ➢ Test questions pertaining to employment examinations
- ➢ Documents pertaining to pending litigation.

Protecting Confidential Information While In Transit

- ➢ Email
- ➢ Removable Media
- ➢ Laptops & Handheld Devices
- ➢ Faxing
- ➢ File Transfers.

Protecting Confidential Information While at Rest

➢ Network Shares

➢ Desktop Workstation

➢ Backup Media.

Protecting Confidential Information

**If You Do Not Require
Confidential Information
Do Not Store or Include in Your Files**

User Agreement Forms

- ➢ CDC 1857 - Appropriate Use
- ➢ CDC 3025 – Annual User Agreement Form
- ➢ CDC 1900 – Non-Employee User Agreement Form

Awareness Training

➢ Required Annually for ALL Staff
who Use or Access Computers

➢ Available on the Intranet at /intranet/infosecurity.

Incident Reporting

Unauthorized Access to, Modification or Destruction of CDCR Information Assets, including:

- ➢ Databases, Data Files and Applications
- ➢ Reports and Documentation
- ➢ Computer Systems and Software
- ➢ Telecommunication Systems
- ➢ Network Services.

How to Report an Incident

Timeframe:

Within three (3) days

Who Reports:

Local ISC

Where Does it Go:

ISO and Your Chain of Command

How to Report:

Reporting Template on Intranet\infosec.

Incident Reporting

- ➢ Inmates using Computers in unauthorized manner
- ➢ Inmates in possession of confidential
  or personal information
- ➢ Unauthorized Access to Information Systems
- ➢ Defacement of Web Pages
- ➢ Denial of Service Attacks
- ➢ Lost or Stolen Computers, including Laptops and PDAs.

Minimizing Damage

➢ No Personal Information on Portable Devices and Removable Media.

➢ Encrypt When Elimination is Not Possible

➢ Do Not Leave Portable Devices Unattended

➢ Use Secure Transfer Protocols for File Movement

➢ Supervise Offenders Using Computers at all Times

➢ Do Not Share Logons and Passwords

➢ Patches and Virus Software Kept Current

➢ Use Network Shares with Appropriate Permissions.

Email Etiquette

➢ Email is NOT Secure
➢ Email is NOT Private

Email Etiquette

Encourage….

➢ Personal Folders On a Network Share
➢ Bulletin Boards for Announcements
➢ Keep it Civil – Drama is for Soap Operas
➢ Accurate and Current Global Address Book.

Email Etiquette

Discourage…

➢ Use of Large Distribution Lists

➢ "Reply All," especially in conjunction with Large Distribution Lists

➢ Blank and Misleading Subject Lines

➢ Including Confidential Information in Email.

Email Etiquette

What to do with Email that have or contain…

➢ Unsolicited information about
degrees, drugs, degenerates, etc. (*SPAM*)

➢ Phishes

➢ Pleas from African Nationalists

➢ Blank and Misleading Subject Lines.

Email Etiquette

- ➢ Keep to the Point
- ➢ No Jokes, Chain Letters, Personal Benefit
- ➢ No Profanity, Pornography, Offensive Content
- ➢ No Politicking
- ➢ No Copyright-Protected Material
- ➢ Personal Email kept to a Minimum.

California
Department of Corrections and Rehabilitation

Questions